Hepting et al v. AT&T Corp. et al Doc. 236

Terry Gross (103878)
Adam C. Belsky (147800)
Monique Alonso (127078)
GROSS & BELSKY LLP
180 Montgomery Street, Suite 2200
San Francisco, California 94104
Telephone: 415-544-0200
Facsimile: 415-544-0201
terry@grossbelsky.com

Micha Star Liberty (215687)
LIBERTY LAW OFFICE
78 First Street
San Francisco, CA 94105-2523
Telephone: 415-896-1000
Facsimile: 415-896-2249

THE CENTER FOR NATIONAL SECURITY STUDIES
Kate A. Martin
1120 19th Street, NW, 8th Floor
Washington, D.C. 20036

Attorneys for Amicus Curiae
THE CENTER FOR NATIONAL SECURITY STUDIES

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

TASH HEPTING, GREGORY HICKS, CAROLYN JEWEL and ERIK KNUTZEN on Behalf of Themselves and All Others Similarly Situated, Plaintiff, v. AT&T CORP., AT&T INC. and DOES 1-20, Inclusive, Defendant.	Case No. C-06-00672 VRW **MEMORANDUM OF AMICUS CURIAE IN OPPOSITION TO THE MOTION BY THE UNITED STATES GOVERNMENT TO DISMISS OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT** Judge: The Hon. Vaughn R. Walker Hearing Date: June 21, 2006 Courtroom: 6, 17th Floor

Dockets.Justia.com

The Center for National Security Studies (the "Center" or "Amicus") respectfully submits this Memorandum of Amicus Curiae in Opposition to the Motion by the United States Government to Dismiss or, in the Alternative, for Summary Judgment (the "Government Motion") and asserts the following grounds in support:

I. INTRODUCTION

The Center is a nonpartisan civil liberties organization in Washington, D.C., that was founded in 1974 to ensure that civil liberties are not eroded in the name of national security. The Center seeks to find solutions to national security problems that protect both the civil liberties of individuals and the legitimate national security interests of the government. For more than 30 years, the Center has worked to protect the Fourth Amendment rights of individuals to be free of unreasonable searches and seizures, especially when conducted in the name of national security. The Center, then affiliated with the American Civil Liberties Union, was asked to testify before Congress when the Foreign Intelligence Surveillance Act ("FISA") was first enacted. In 1994, when Congress amended the Act to include physical searches, Kate Martin, Director of the Center, was again asked to testify. Over the years, the Center has also filed several amicus briefs and lawsuits concerning the lawfulness of FISA surveillance.

II. SUMMARY OF ARGUMENT

Plaintiffs have brought claims against AT&T under, inter alia,[1] certain provisions of the Federal Intelligence Surveillance Act, 50 U.S.C. § 1801, et seq. ("FISA") and the Stored Communications Act, 18 U.S.C. § 2701, et seq. ("SCA"). This brief will focus on plaintiffs' claims that AT&T disclosed millions of records – either in real time or after the fact – detailing the numbers called by AT&T subscribers and the numbers of the calls they received without meeting the requirements of FISA or the SCA.[2] Congress intended that plaintiffs be afforded the opportunity to challenge such violations of

[1] Amicus does not, in this Memorandum, address all the claims raised by plaintiffs and arguments raised by the Government. Rather, Amicus here demonstrates that a careful analysis of the claims is required and that, at a minimum, certain claims cannot be dismissed at this stage of the litigation. Nevertheless, Amicus notes that the claims not addressed in this Memorandum appear to raise serious issues of statutory and constitutional violations by AT&T.

[2] While Amicus believes that the Terrorist Surveillance Program described by the President and any broader electronic surveillance outside of the FISA warrant provisions is illegal, in the limited amount of time available to Amicus, this Memorandum does not address those issues.

these statutes. Furthermore, the legality of the disclosure of customer records can be litigated without disclosure of state secrets. The case does not need to involve any description of the design or operation of the government's surveillance programs, but instead can focus entirely on the legality of the actions of defendant AT&T.

III. ARGUMENT

A. Congress Provided a Private Right of Action for both FISA and SCA Violations, and Congress Would Not Create A Private Right of Action That is Completely Illusory.

Both FISA and SCA regulate the disclosure of customer records to the government. The FISA provides the exclusive means for obtaining call records for foreign intelligence purposes in real-time through the use of pen register and trap and trace devices. 50 U.S.C. § 1842; 18 U.S.C. § 2511(2)(f). The SCA provides for the disclosure of historic call records under certain circumstances. 18 U.S.C. §§2702 - 2703. Both statutes establish specific requirements for the disclosure of records. Plaintiffs allege in this case that AT&T has violated the statutes by failing to comply with these requirements.

Congress created private rights of action for violations of both FISA and SCA. 50 U.S.C. §1810; 18 U.S.C. §2707; *see also* 18 U.S.C. § 2520. The FISA provides for the recovery of actual damages, punitive damages, and reasonable attorney's fees and other investigation and litigation costs incurred. 50 U.S.C. §1810. The relief available to plaintiffs for violations of SCA provisions includes equitable and declaratory relief, damages, punitive damages and attorney's fees. 18 U.S.C. §2707; *see also* § 2520

Both statutes regulate governmental intelligence-gathering activities. Indeed, FISA involves a single topic: foreign intelligence information, including the means by which the government may lawfully obtain it through electronic surveillance.[3] Accordingly, any lawsuit brought under 50 U.S.C. § 1810 necessarily "implicates" foreign intelligence.

Similarly, Congress knew that lawsuits brought under the SCA might well involve intelligence

[3] "Foreign intelligence information" is broadly defined as information pertaining to the ability of the United States to defend against attack, the national defense, the security of the United States, and the foreign affairs of the United States. 50 U.S.C. § 1801(e).

information.[4] For example, the SCA contains specific provision for turning over records to the FBI that are "relevant to an authorized investigation to protect against *international terrorism or clandestine intelligence activities*..." on the basis of a certification by certain designated FBI officials. 18 U.S.C. § 2709 (emphasis added).

Except under specified conditions, the SCA prohibits and sanctions by fine and imprisonment unauthorized access to or disclosure of customer records. 18 U.S.C. §§ 2701-02. Sections 2703 and 2709 set out the only conditions – including subpoena, warrant or court order – under which a governmental entity may require a communications provider to turn over records. 18 U.S.C. §§ 2703(c) & 2709. At the same time, the SCA contains many exclusions to its otherwise broad prohibitions against telephone companies' intercepting wire or electronic communications or turning over customer records. For example, section 2702(a), which forms a part of plaintiffs' claims here, begins, "Except as provided in subsection (b) or (c) ...." 18 U.S.C. § 2702(a). Subsections (b) and (c) respectively list 8 and 6 subparts of exceptions. Similarly, SCA section 2707, which affords a civil damages remedy to anyone aggrieved by unauthorized access or disclosure, also provides a number of specific "complete defense[s]" to such an action.[5]

By laying down specific conditions under which the government may access customers' records for intelligence purposes in the same law that provides an aggrieved customer with a civil remedy for unauthorized access or disclosure, Congress clearly meant to allow a civil suit to proceed when those conditions have not been met. Congress should not be found to have created a civil damages remedy for unauthorized disclosure of customer records that can be rendered nugatory by the invocation of a common law privilege. The Court should strive to avoid such an anomaly.

In 1958, the Second Circuit faced a similar situation under the Invention Secrecy Act (ISA), which allowed the patent office to withhold a patent grant for inventions implicating national security concerns. 35 U.S.C. §§ 181-188 ("ISA"). *See Halpern v. United States*, 258 F.2d 36 (2d Cir. 1958).

---

[4] *See, e.g.*, 18 U.S.C. § 2511(2)(a)(ii) ("providers of wire or electronic communication service . . . are authorized to provide information . . . to persons authorized by law to intercept wire, oral or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act ....").

[5] For example, a defendant can show that it relied in good faith on "a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization ...." 18 U.S.C. § 2707(e)(1).

Under the ISA, inventors were compensated for the loss of the income resulting from the withholding of the patent grant. *Id.* at 38-39.

The ISA also allowed inventors to bring suit in federal court for payment of the compensation if their claim was denied in the administrative procedure set up by the statute. *Id.* at 40. Inventor Halpern claimed compensation under the ISA, but the claim was denied. *Id.* at 37. He then sued in federal court, as contemplated by the ISA. *Id.* at 38, 41. As in this case, the government claimed that its invocation of the state secret privilege required dismissal of the plaintiff's entire case. *Id.* at 41.

The trial court dismissed Halpern's claims, but the Second Circuit reversed, for reasons that apply equally to the facts before this Court:

> Congress has created rights which it has authorized federal district courts to try. Inevitably, by their very nature, the trial of cases involving patent applications placed under a secrecy order will always involve matters within the scope of this [state secrets] privilege. *Unless Congress has created rights which are completely illusory, existing only at the mercy of Government officials, the act must be viewed as waiving the privilege.*

Id. at 43 (emphasis added). The court added "[o]f course, any such waiver is dependent upon the availability and adequacy of other methods of protecting the overriding interest of national security during the course of a trial." *Id.* at 43. It then permitted the district court to hold a trial *in camera* "in which the privilege relating to state secrets may not be availed of by the United States" provided that the trial could be carried out without substantial risk of publicly divulging secret information. *Id.* at 44.

Amicus respectfully suggests that this Court should not presume Congress created a private right of action that is "completely illusory," as the private right of action under both FISA and the SCA would be if the federal government could immediately gain dismissal of all such suits by claiming that evidence of violations is a privileged state secret. Instead, the Court should seek ways to assure that plaintiffs can pursue the rights granted to them by Congress.

//

//

//

B. The Government's Conclusory Statements In Support of Invocation of the Privilege Do Not Establish any Danger of Disclosure of State Secrets Here.

In *United States v. Reynolds*, 345 U.S. 1, 8 (1953), the Supreme Court stated that the state secret privilege "is not to be lightly invoked." *Id.* at 9-10. A "court must not merely unthinkingly ratify the executive's assertion of absolute privilege, lest it inappropriately abandon its important judicial role." *In re United States*, 872 F.2d 472, 475 (D.C. Cir. 1989). "Judicial control over the evidence in a case cannot be abdicated to the caprice of executive officers." Furthermore, "[w]here there is a strong showing of necessity, the claim of privilege should not be lightly accepted," *Reynolds*, 345 U.S. at 11.

The claim has to be specific. In *Ellsberg v. Mitchell*, 709 F.2d 51 (D.C. Cir. 1983), the appellate court found that the government had not properly explained how disclosing identities of the attorneys general who authorized wiretaps might affect national security. The court remanded so the government would give a sufficient and specific explanation. There had been public disclosure of the wiretaps, so that a more specific explanation was necessary by the government as to the *harm* of disclosure in the lawsuit. *Id.* at 61-63 (noting that the harm was not "self-evident").

> The more specific the public explanation, the greater the ability of the opposing party to contest it. The ensuing arguments assist the judge in assessing the risk of harm posed by dissemination of the information in question. This kind of focused debate is of particular aid to the judge when fulfilling his duty to disentangle privileged from non-privileged materials -- to ensure that no more is shielded than is necessary to avoid the anticipated injuries.

Id. at 63.

Therefore, the court held that the trial court should insist (1) that the formal claim of privilege be made on the public record and (2) that the government either (a) publicly explain in detail the kinds of injury to national security it seeks to avoid and the reason those harms would result from revelation of the requested information or (b) indicate why such an explanation would itself endanger national security. *Id.* at 63.

In response to plaintiffs' need for the core information as to whether AT&T turned customer records over to the government without meeting the requirements imposed by statute, the government submits only the vaguest and most conclusory statements. For example, the Negroponte Declaration makes only a single reference to AT&T. Negroponte Declaration ¶12. That paragraph, however, gives not a clue as to what activities of AT&T Mr. Negroponte is referring to and does not even specifically claim a state secrets privilege as to "NSA's purported involvement with AT&T." *Id.*

The only other evidence submitted by the government on plaintiffs' crucial factual allegation consists of a single paragraph, ¶8, in the Alexander Declaration. That paragraph, however, adds nothing to the record. It merely repeats, virtually verbatim, some of the allegations in Negroponte Declaration ¶12.

In sum, the Negroponte and Alexander Declarations fall far short or the showing the government needs to make.

- Use of the vague phrases such as "these sorts of allegations" and "these matters" does not afford this Court any guidance as to which of plaintiff's allegations the affiants are talking about.
- Negroponte Declaration ¶12 and Alexander Declaration ¶8 make no contentions whatsoever about the core factual allegation that AT&T handed customer records over to the government.
- Specifically, Negroponte Declaration ¶12 and Alexander Declaration ¶8 fail to claim that the core fact alleged, that is, whether or not AT&T handed customer records over to the government without meeting the requirements imposed by statute, is (a) a state secret; (b) "intelligence information"; or (c) the kind of fact the government can neither confirm nor deny.

In any event, the crucial fact – whether or not AT&T provided customer telephone records to the government without meeting the requirements imposed by statute – scarcely seems capable of constituting a state secret. First, the SCA and the FISA obviously contemplate that under appropriate circumstances telephone companies will provide customer records to the government. 18 U.S.C. §§ 2702 - 2703 & 50 U.S.C. § 1842. Nor is it a secret that the government is targeting al Qaeda communications; the government has acknowledged this. There can be no reasonable danger to the national security to reveal that the government acquired customer records as part of its campaign against al Qaeda.[6] Disclosure of the approximate number of records provided to the government also cannot

[6] This is not a situation where merely acknowledging the existence of a surveillance program might harm the national security, e.g. by alienating foreign governments.

reasonably endanger national security because it reveals nothing about how those records are used to investigate the relatively few people who are suspected terrorists.

Second, the issue of whether the government met the statutory requirements and gave AT&T the necessary certification under 18 U.S.C. § 2511(2)(a)(ii) does not require disclosure of state secrets. The existence of a certification would indicate that AT&T provided records, but revelation of that fact by itself would not endanger national security. The non-existence of a certification, which would suggest that AT&T was not authorized to provide records, also cannot constitute a state secret. The possibility that AT&T acted *illegally* by providing records affords no additional information about the design or operation of any surveillance program and therefore cannot damage national security.

Finally, the government's argument that the plaintiffs' standing cannot be determined without disclosure of secret information that would endanger national security is highly implausible. Plaintiffs allege that AT&T has disclosed millions of customer records to the government. As noted, this fact, if true, does not endanger national security because it discloses nothing about the design or operation of any government program. Yet this fact would have a crucial impact on the standing issue. It would make it likely almost to a certainty that many of the plaintiffs have had their records disclosed and thus are aggrieved persons under FISA and SCA. And if the records of massive numbers of people have been similarly disclosed there can be no reasonable danger that the national security will be harmed by requiring the government to acknowledge that one or a handful of plaintiffs have had their records disclosed. Such an acknowledgment would not enable the plaintiffs to know that they, as opposed to the millions of other aggrieved subscribers, were the targets of any government investigation. *Cf. Halkin v. Helms*, 690 F.2d 977 (D.C. Cir. 1982) (discussing the danger of disclosing the names of people on a government watchlist).

At later stages of this litigation – *e.g.*, a hearing on damages – the Court can use its inherent powers to conduct proceedings *in camera* if there is any risk of disclosure that would endanger national security.[7] That some difficult issues with respect to disclosure may arise at a later stage of these proceedings provides no basis for granting a motion to dismiss or for summary judgment now.

[7] The Court of Appeals for the District of Columbia has suggested that the procedures of 50 U.S.C. § 1806(f) permitting *in*

IV. CONCLUSION

For the reasons stated above, Amicus respectfully suggests that no reason exists to dismiss this case at this stage of the litigation. Therefore, the Government Motion to Dismiss, or in the Alternative, for Summary Judgment on the state secrets privilege should be denied.

Dated: June 16, 2006

Respectfully submitted,

Terry Gross (103878)
Adam C. Belsky (147800)
Monique Alonso (127078)
GROSS & BELSKY LLP
180 Montgomery Street, Suite 2200
San Francisco, CA 94104
Telephone: (415) 544-0200
Facsimile: (415) 544-0201
terry@grossbelsky.com

By: //s// Terry Gross
Terry Gross

Micha Star Liberty (215687)
LIBERTY LAW OFFICE
78 First Street
San Francisco, CA 94105-2523
Telephone: 415-896-1000
Facsimile: 415-896-2249

Kate A. Martin
Brittany Benowitz
THE CENTER FOR NATIONAL SECURITY STUDIES
1120 19th Street NW, 8th Floor
Washington, D.C. 20036
Telephone: (202) 721-5620

Attorneys for Amicus Curiae
THE CENTER FOR NATIONAL SECURITY STUDIES

---

camera and *ex parte* review may be used in suits such as this under § 1810. *See ACLU v. Barr,* 952 F.2d 457, 470 (D.C. Cir. 1991); *but see* Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure*, § 5666, 629-31 (1992) (describing need for adversary hearing to evaluate claim of state secrets privilege).

OF COUNSEL

Joseph N. Onek
Patricia M. Wald
1120 19th Street NW, 8th Floor
Washington, D.C. 20036
Telephone: (202) 721-5600
Fax: (202) 530-0128

CERTIFICATE OF SERVICE

I hereby certify that the foregoing MEMORANDUM IN OPPOSITION TO THE MOTION TO DISMISS, OR IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT BY THE UNITED STATES OF AMERICA will be served by means of the Court's CM/ECF system, which will send notifications of such filing to the following:

Peter D. Keisler
Assistant Attorney General, Civil Division
Carl J. Nichols
Deputy Assistant Attorney General
Douglas N. Letter
Terrorism Litigation Counsel
Joseph H. Hunt
Director, Federal Programs Branch
Anthony J. Coppolino
Special Litigation Counsel
Andrew H. Tannenbaum
Trial Attorney
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, D.C. 20001

Cindy Cohn
Lee Tien
Kurt Opsahl
Kevin S. Bankston
Corynne McSherry
James S. Tyre
545 Shotwell Street
San Francisco, CA 94110

Reed R. Kathrein
Jeff D. Friedman
Shana E. Scarlett
Lerach, Coughlin Stoia Geller Rudman & Robbins LLP
100 Pine Street, Suite 2600
San Francisco, CA 94111

Bert Voorhees
Theresa M. Traber
Traber & Voorhees
128 North Fair Oaks Avenue, Suite 204
Pasadena, CA 91103

Bruce A. Ericson
David L. Anderson
Partick S. Thompson
Jacob R. Sorensen
Brian J. Wong
Pillsbury Winthrop Shaw Pittman LLP
50 Freemont Street
PO Box 7880
San Francisco, CA 94120-7880

David W. Carpenter
Bradford Berenson
Edward R. McNicholas
David L. Lawson
1501 K. Street, NW
Washington, DC 20005

//s//_Mary B. Cunniff